

**IN THE UNITED STATES DISTRICT COURT  
FOR DISTRICT OF MONTANA**

**IN THE MATTER OF THE  
SEARCH OF:**

**Samsung Galaxy brand cell phone,  
model J7 Crown, SM-S767VL,  
IMEI: 356823096116517.**

**Case No. MJ-22-20BLG-TJC**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR  
A WARRANT TO SEARCH AND SEIZE**

I, Jon Mathew N Poe, a United States Postal Inspector (USPI) Task Force Officer with EMHIDTA, being duly sworn, state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Fed. R. Crim. P. 41 for a search warrant authorizing the search of a Samsung Galaxy brand cell phone, model J7, SM-S767VL Crown, IMEI: 356823096116517, further described in Attachment A. The Device is currently located at the EMHIDTA Office, Billings, MT.

2. The applied for search warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

3. I, Jon M. Poe, am currently a Postal Inspector Task Force Officer (TFO) for the United States Postal Inspection Service through the Eastern Montana High Intensity Drug Trafficking Area Task Force (EMHIDTA). This appointment started on December 2, 2021. I have been employed full time with the Yellowstone

County Sheriff's Office since December 2009. I received a bachelor's degree from Montana State University-Billings. I attended the Montana Law Enforcement Academy in the winter of 2010. Currently, I am assigned to the EMHIDTA Narcotics Unit where I investigate the distribution of dangerous drugs. Prior to this assignment, I worked three years as a School Resource Officer (SRO), approximately six years as a patrol officer, and served approximately two years on deployment status as a commissioned officer with the US Army.

4. As a Postal Inspector TFO, I investigate to prevent the flow of illicit drugs and contraband through the United States Mail. I have assisted with investigations involving the distribution of controlled substances. I have also participated in narcotics investigations which have resulted in the seizure of large quantities of controlled substances such as cocaine, methamphetamine, and heroin. I am familiar with and have participated in all of the normal methods of investigation, including but not limited to visual surveillance, questioning of witnesses, the use of search and arrest warrants, and the use of informants. Additionally, I have consulted with other agents who have been involved in similar investigations.

5. I have participated in investigations involving the interception of wire communications and the use of video surveillance. I am familiar with the manner in which narcotics traffickers and money launderers conduct their operations, including but not limited to: their methods of importing and distributing controlled substances, use of telecommunication devices to include cellular telephones, use of counter surveillance techniques, and use of numerical codes and coded and/or cryptic language, words, and references to conduct their transactions.

6. This affidavit is based upon information I have gained through training and experience, as well as upon information provided to me by other individuals, including law enforcement officers.

7. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known concerning this investigation but have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence relating to violations of 21 U.S.C. § 841(a)(1) and 21 U.S.C. § 846, including contraband, fruits of one or both crimes, and property used or intended to be used in the commission of one or both crimes, are located within a Samsung brand cell phone, serial number IMEI: 356823096116517 (model not accessible), further described in Attachment A. The Device is currently located at the EMHIDTA Office, Billings, MT.

8. I am familiar with the facts and circumstances of this investigation, as set forth in this affidavit, as a result of the following: (1) my training and experience; (2) my personal involvement in this investigation; (3) my discussions with other federal, state, and local law enforcement familiar with this investigation; (4) my review of reports and other documents prepared by federal and local law enforcement officers; (5) physical surveillance conducted by federal agents or local law enforcement agencies, which has been reported to me either directly or indirectly.

### **TECHNICAL TERMS**

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. **Data:** means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.
- c. **Email or electronic mail:** means messages transmitted over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, computer networks, and minicomputers have an email system. Sent messages are stored in electronic mailboxes at least until the recipient retrieves them. After reading electronic mail, recipients can store it on their computer as a file, forward it to other users, or delete it, or they may store the message on a remote server, such as the one from which they may have retrieved the email.

- d. **Image or copy:** refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but attributes may change during the reproduction.
  - e. **Internet:** is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
  - f. **Text Messages:** are a form of communication through the use of cellular telephones or handheld electronic devices upon an electronic service provider’s network or system. A message normally contains text composed by the sender, usually input via a lettering system on the device or computers keypad. The message can also be an image or short video sent or received.
  - g. **Uniform Resource Locator:** (URL) *are typically used to access web sites or other services on remote devices such as <http://www.usdoj.gov>, for example.*
  - h. **Voice Mail:** means a computerized system for answering incoming phone calls and allowing the caller to leave a message, which may be later retrieved.
  - i. **World Wide Web:** can be considered a massive database of information that is stored on linked computers that make up the Internet. This information can be displayed on a computer in the form of a web page, which is a document on the World Wide Web. A web site is a related collection of files and can consist of any number of web pages.
10. Based on my training, experience, and research, I know that smartphone devices, such as the Devices, have capabilities that allow them to serve as a wireless

telephone, data storage device, and digital camera and that smartphone devices can connect to the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, who the user was communicating with, and the content of those communications. I also know the devices would allow to store text messages and digital images of, or related to, the possession or distribution of controlled substances or firearms.

11. Based upon my knowledge, training, and experience in investigating federal narcotics crimes, and the experience and training of other law enforcement officers with whom I have had discussions, I am aware of the following:

#### **EXAMINATION OF ELECTRONICAL INFORMATION**

12. The examination of the device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the United States needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant.

13. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders responsive to this search warrant do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the



purview of the warrant relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

14. If the examination does not reveal any data falling within the scope of the warrant, the United States will seal any non-responsive information, absent further authorization from the Court.

15. The United States will retain a forensic image of all of the electronic information produced during the examination of the device to prove the authenticity of evidence to be used at trial, to respond to questions regarding the corruption of data, to establish a chain of custody of data, to refute claims of fabricating, tampering, or destroying data, and to address potential exculpatory evidence claims where, for example, a defendant claims that the United States avoided its obligations by destroying data or returning it to a third party.

### **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION**

16. It is not possible to determine, merely by knowing the smartphone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Smartphone devices today can be simple cellular telephones and text message devices, and/or they can include cameras, serve as personal digital assistants and have functions such as calendars and full address books, and/or they can be mini-computers

allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the devices may only be powered in a secure environment or, if possible, started in “airplane mode,” which disables access to the network. Unlike typical computers, many smartphones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some smartphone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive.

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, items



that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), I seek permission for an agent review of the device as well as the forensic examination of the device consistent with the warrant. The examination will require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. In searching the data stored on the device, law enforcement personnel executing this search warrant will employ the following procedure:

- a. The team searching the device will do so only by using search protocols specifically chosen to identify only the specific items to be seized described in Attachment B.
- b. The team may subject all of the data contained in the device or the forensic copy to the protocols to determine whether the device and any data falls within the items to be seized described in Attachment B. The team searching the device may also search for and attempt to recover “deleted,” “hidden” or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized described in Attachment B.

- c. These search protocols also may include the use of tools to exclude normal operating system files and standard third-party software that do not need to be searched.
- d. When searching the device pursuant to the specific search protocols selected, the team searching the device shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.
- e. If the team searching the device pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.
- f. At the conclusion of the search of the device, any one device determined to be itself an instrumentality of the offense(s) and all the data thereon shall be retained by the United States until further order of the Court or one year after the conclusion of the criminal case/investigation.
- g. Notwithstanding, after the completion of the search of the device, the United States shall not access digital data falling outside the scope of the items to be seized in this warrant on any retained device or digital data absent further order of Court.
- h. If the search team determines that a device is not an instrumentality of any offense under investigation and does not contain any data falling within the list of items to be seized described in Attachment B, the United States will as soon as practicable return the device and delete or destroy all the forensic copies thereof.
- i. If the search determines that the device or the forensic copy is not an instrumentality of any offense under investigation but does contain data falling within the list of the items to be seized described in

Attachment B , the United States either (i) within the time period authorized by the Court for completing the search, return to the Court for an order authorizing retention of the device and forensic copy; or (ii) retain only a copy of the data found to fall within the list of the items to be seized described in Attachment B and return the device and delete or destroy all the forensic copies of the device.

### **PROBABLE CAUSE**

20. The information contained in this Affidavit is based upon information provided by other HIDTA agents, state and local law enforcement officers, public source documents, and my own personal investigation. The information presented in this Affidavit is intended to demonstrate probable cause and does not set forth all of the information I have become familiar with in this investigation.

21. On January 12, 2022, Agents of the Eastern Montana High Intensity Drug Trafficking Areas (EMHIDTA) was interviewing a source of information (SOI). The SOI provided information Malea ORSER had made a trip to Denver, CO and purchased 1000 fentanyl pills and two pounds of methamphetamine and transported the drugs back to the Billings Area.

22. The SOI was with ORSER on January 11, 2022 and stated she had sold all the pills and had a small amount of methamphetamine left in her possession.

23. The SOI stated ORSER was planning on returning to Denver, CO in order to purchase 4,000 pills and transport the drug back to the Billings area. The SOI stated ORSER had recently purchased a 2008 Ford Taurus (MT PLT: 3-78337D). The SOI stated the vehicle was not in good working order and would not make it to Denver, CO because of mechanical issues.

24. TFO Poe discovered through information obtained from a Facebook search warrant, Orser was suspected of living at 641 Hillview Ln. TFO Poe located

the Ford Taurus at this address. This address is owned by Justin Goselin and his brother's truck was in the driveway. His brother is Taylor GOSELIN. Taylor GOSELIN is on Malea ORSER's friend's list on her Facebook profile.

25. During an interview with GOSELIN, he stated he has known Malea ORSER for years and once dated her.

26. TFO Poe has discovered through information obtained through a Facebook search warrant, electronic conversations between ORSER and multiple individuals, regarding the purchase and sales of illegal drugs in the Billings, MT area.

27. Agents of HIDTA learned through a subpoena served to Enterprise car rental, Taylor GOSELIN rented a four door, 2021 Chevy Malibu, black in color bearing Oregon License plates 256MJM. With VIN: 1G1ZD5ST6MF004324.

28. An application for a Pen and Trap search warrant for Malea ORSER's Verizon cell phone (406-591-2623) was submitted and granted by the Honorable District Judge Jessica Fehr on 13 January 2022.

29. On 01/14/2022, TFO Poe received GPS information showing Malea ORSER's phone was traveling towards Denver, CO. TFO Poe monitored GPS information as it was received from Verizon Wireless and observed ORSER's phone was in the Castle Rock, CO area throughout the weekend (01/15/2022-01/16/2022)

30. On or around 01/14/2022, a second SOI confirmed with Agents of HIDTA, ORSER was in Denver, CO.

31. On 01/16/2022, HIDTA agents were contacted and informed Malea ORSER was returning to the Billings, MT area. A Yellowstone County Sheriff's Office Deputy was provided information regarding Malea ORSER and the vehicle she was traveling in.

32. An agent of HIDTA passed the suspect vehicle and reported a female was a passenger in the vehicle. The suspect vehicle had Oregon plates.

33. Based on the information agents of HIDTA had obtained from the SOI, the conversations discovered by TFO Poe involving the purchase and sales of drugs in the Billings area by Malea ORSER and the description of the suspect matching the information reported to agents of HIDTA, a traffic stop was conducted based on probable cause.

34. Taylor GOSELIN (05/03/1995), Matthew SHELHAMER (11/01/1994), and Malea ORSER (11/22/1997) were identified in the vehicle. SHELHAMER was in the front passenger seat, GOSELIN was driving and ORSER was in the back seat.

35. Based on the automobile exception to the warrant requirement, agents decided to search the vehicle. A small silver container with a second container chained to it was located behind the back trunk liner, on the driver side towards the front corner. Inside the small silver container agents located multiple pills that appeared to be fentanyl. They had M30 printed on the pills. This print on the pill is common for fentanyl pills.

36. A lock box was located in the rear trunk on the driver side. The lock box had a magnet on it, and it was fixed to the interior of the metal back driver side fender. ORSER had the key to the lock box on her person. The lock box was opened and inside the box was a large amount of suspected methamphetamine, a ball of a brown substance which is suspected to be heroin and a large amount of suspected fentanyl pills. A blue transparent pen was in the lock box and it contained more fentanyl pills.

37. In the front passenger floorboard, ten pens were located on the floorboard and inside those pens were more fentanyl pills.

38. Four phones were located within the vehicle. A black Iphone with a dirty screen protector was located in the center console, an Iphone with a clear case with flowers print was located in the back seat and a white Iphone (model A1660) was located on the front passenger seat.

39. The Samsung Galaxy brand cell phone, model J7, SM-S767VL Crown, IMEI: 356823096116517 was located in the back seat where Malea ORSER was sitting. The phone was unlocked and when TFO Poe placed the phone in airplane mode, TFO Poe noticed there was no SIM card in the phone.

40. Because of the high number of vehicles passing our location which included multiple semi's, the vehicle was secured and transported to the Billings Police Department Evidence Facility in order to conduct a thorough search.

41. SHELHAMER and ORSER were placed under arrest for active warrants and transported to the Yellowstone County Sheriff's Detention Facility (YCDF). GOSELIN was released from the scene and A Montana Highway Patrol (MHP) trooper drove him away from the scene.

42. A zip lock baggy containing a large number of suspected fentanyl pills was located on SHELHAMER's person at YCDF.

43. TFO Poe has read multiple Facebook messages from Malea ORSER's account discussing the sale and purchase of illegal drugs.

44. Your affiant believes there is probable cause to show that Malea ORSER has been involved in a drug trafficking organization responsible for distributing large quantities of drugs within the District of Montana and other locations. Your affiant further believes that ORSER has used a cellular device in




furtherance of the drug trafficking activity, both in speaking about currency exchanged for illegal drugs, and in speaking about her travels. Furthermore, your affiant believes there is probable cause to conduct a search of the cellular devices ORSER had in her possession on January 16, 2022, when she was found to be in possession of methamphetamine, fentanyl, and heroin.

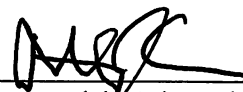
**CONCLUSION**

46. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

RESPECTFULLY SUBMITTED:

  
\_\_\_\_\_  
Jon Poe  
Postal Inspector TFO  
United States Postal Inspector Service  
EMHIDTA

Subscribed and sworn to before me on this 2 day of February, 2022.

  
\_\_\_\_\_  
Honorable Timothy J. Cavan  
United States Magistrate Judge